TANBIR 01738359555

কম্পিউটার ভাইরাস

কম্পিউটার ভাইরাস হল এক ধরনের কম্পিউটার প্রোগ্রাম যা ব্যবহারকারীর অনুমতি বা ধারণা ছাড়াই নিজে নিজেই কপি হতে পারে। মেটামর্ফিক ভাইরাসের মত তারা প্রকৃত ভাইরাসটি কপিগুলোকে পরিবর্তিত করতে পারে অথবা কপিগুলো নিজেরাই পরিবর্তিত হতে পারে। একটি ভাইরাস এক কম্পিউটার থেকে অপর কম্পিউটারে যেতে পারে কেবলমাত্র যখন আক্রান্ত কম্পিউটারকে স্বাভাবিক কম্পিউটারটির কাছে নিয়ে যাওয়া হয়। যেমন: কোন ব্যবহারকারী ভাইরাসটিকে একটি নেট ওয়ার্কের মাধ্যমে পাঠাতে পারে বা কোন বহনযোগ্য মাধ্যম যথা ফ্লপি ডিস্ক, সিডি, ইউএসবি ড্রাইভ বা ইন্টারনেটের মাধ্যমে ছড়াতে পারে। এছাড়াও ভাইরাসসমূহ কোন নেট ওয়ার্ক ফাইল সিস্টেমকে আক্রান্ত করতে পারে, যার ফলে অন্যান্য কম্পিউটার যা ঐ সিস্টেমটি ব্যবহার করে সেগুলো আক্রান্ত হতে পারে। ভাইরাসকে কখনো কম্পিউটার ওয়ার্ম ও ট্রোজান হর্সেস এর সাথে মিলিয়ে ফেলা হয়। ট্রোজান হর্স হল একটি ফাইল যা এক্সিকিউটেড হবার আগ পর্যন্ত ক্ষতিহীন থাকে।

বর্তমানে অনেক পার্সোনাল কম্পিউটার (পিসি) ইন্টারনেট ও লোকাল এরিয়া নেটওয়ার্কের সাথে যুক্ত থাকে যা ক্ষতিকর কোড ছড়াতে সাহায্য করে। ওয়ার্ল্ড ওয়াইড ওয়েব, ই-মেইল ও কম্পিউটার ফাইল শেয়ারিং এর

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

T@NB!R 01738359555
মাধ্যমে ভাইরাস সংক্রমন ঘটতে পারে। কিছু ভাইরাসকে তৈরি করা হয় প্রোগ্রাম ধ্বংশ করা, ফাইল মুছে ফেলা বা হার্ড ডিস্ক পূণর্গঠনের মাধ্যমে কম্পিউটারকে ধ্বংশ করার মাধ্যমে। অনেক ভাইরাস কম্পিউটারের সরাসরি কোন ক্ষতি না করলেও নিজেদের অসংখ্য কপি তৈরি করে যা লেখা, ভিডিও বা অডি ও বার্তার মাধ্যমে তাদের উপস্থিতির বহিঃপ্রকাশ ঘটায়। নিরীহ দর্শন এই ভাইরাসগুলোও ব্যবহারকারীর অনেক সমস্যা তৈরি করতে পারে। এগুলো স্বাভাবিক প্রোগ্রামগুলোর প্রয়োজনীয় মেমোরি দখল করে। বেশ কিছু ভাইরাস বাগ তৈরি করে, যার ফলশ্রুতিতে সিস্টেম ক্র্যাশ বা তথ্য হারানোর সম্ভাবনা থাকে।

.ভাইরাস কিঃ কম্পিউটারের ভাইরাস কি প্রশ্ন করলে একজন অদক্ষ লোক ও বলে দিতে পারবে এটি কম্পিউটারের শত্রু।এর থেকে দূরে থাকা দরকার।তবে এর মাধ্যমে পুরো উত্তরটা মনে হয় আসবেনা।কম্পিউটার দুটো জিনীসের সমন্বয়ে চলে একটি হার্ডওয়ার অন্যটি সফটওয়ার।আপনি যখন পুরো কম্পিউটারটি হার্ডওয়ার দিয়ে চলার উপযুক্ত করবেন তখন প্রয়োজন হবে অপারেটিং সিস্টেম,মাল্টিমিডিয়া,গ্রাফিক্স,ইউটিলিটি ইত্যাদি সফটওয়ারের যা ছাড়া আপনি কম্পিউটারটা ব্যবহার করতে পারবেনা।ভাইরাস ও সে রকম ১টি সফটওয়ার।তবে সামান্য পার্থক্য আছে। মাল্টিমিডিয়া,গ্রাফিক্স,ইউটিলিটি সফটওয়ার গুলো আপনি আপনার প্রয়োজন পুরণ করার জন্য ব্যবহার

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

T@NB!R 01738359555
করে থাকেন।যে প্রোগ্রামার এটি তৈরি করুক না কেন এটি আপনি যখন ইন্সটল করবেন তখন থেকে আপনার কমান্ডমত এটি কাজ করবে।ভাইরাস কিন্তু আপনার কমান্ডমত কাজ করেনা।এটি যে প্রোগ্রামার তৈরি করে তার কাজ করে।আর ঐ প্রোগ্রামার তার বিভিন্ন উদ্দেশ্য সাধনের জন্য এগুলো তৈরি করে থাকে।এটি এমন এক সফটওয়ার যা ইউজারকে ফাকিঁ দিয়ে নিজে নিজে ইন্সটল হয়ে যায় এবং অল্প সময়ে পুরো কম্পিউটারের নিয়ন্ত্রণ নিয়ে ফেলে।পরে প্রোগ্রামারের উদ্দেশ্যে পূরণ করতে থাকে যার ফলাফল একজন ইউজারের সর্বনাশ।

২.কিভাবে আসেঃ

কিভাবে এই সম্মানিত মেহমান কম্পিউটারে আসে তা বলার আগে কিভাবে এটি ছড়াই বললে মনে হয় আরো পরিস্কার হবে বিষয়টা।আপনাকে যদি কেউ প্রশ্ন করে বর্তমান বিশ্বে তথ্য আদান প্রদানের সবচেয়ে দ্রুত মাধ্যম কোনটি আপনি নিশ্চয় ইন্টারনেট ছাড়া অন্য কিছুর নাম বলবেন না।কারণ চিঠি পত্রের যুগ এখন শেষ পর্যায়ে।আপনি একটা চিঠি পাঠাবেন আমেরিকায় তার জন্য আপনি এখন আর পোষ্ট অফিসে যাননা।কারণ আপনার ইন্টারনেট আছে।একই ভাবে আপনার একটা সফটওয়ার দরকার যেটা আজকেই বের হয়েছে কিছুক্ষণ আগে আমেরিকায়।তাহলে আপনি মার্কেটে গিয়ে হাজার টাকা দিলে ও সেটি পাবেন না।এর জন্য ও আপনার ভরসা ইন্টারনেট।টেক্সট,ইমেজ,অডিও,ভিডিও সব কিছুই আজ ইন্টারনেটের মাধ্যমে পাওয়া যায় যেখানে

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

T@NB!R 01738359555
ভাইরাসটাও একটি।নিচে দুটি উদাহরণ দিচ্ছি।

১.Mr. A

একজন ভাইরাস প্রোগ্রামার।ভাইরাস তৈরি করা এবং ছড়ানোই তার কাজ।উদ্দেশ্য সফল করার জন্য নিজের ব্লগ আছে।আবার সে বিভিন্ন ফোরামের সদস্য এবং সে নিয়মিত ওগুলোতে পোষ্ট করে,সদস্যদের সমস্যাই নিজে কমেন্টস করে।
নতুন ভাইরাসতো তৈরি করেই,যে সব সফটওয়ারগুলোর সিরিয়াল কী পাওয়া যায়না কিন্তু খুব গুরুত্বপূর্ণ সেগুলোর পেচও তৈরি করে যেখানে তার ভাইরাস প্রোগ্রামের কমান্ডগুলো এড করে দেয়।আজকাল পিসিকে স্মুথলি চালানোর জন্য,ট্রাবলশুটিং করার জন্য অনেক গুরুত্বপূর্ণ ইউটিলিটি সফটওয়ার বের হচ্ছে।এসব সফটওয়ারগুলোকে এডিট করে সে নিজের ভাইরাস প্রোগ্রামের কমান্ডগুলো এড করে দেয়(ভাইরাস এফেক্টেড সফটওয়ার)।মোট কথা যে সব সফটওয়ার ও সিরিয়ালের খুব বেশি চাহিদা সেখানে সে সাধ্যমত সব চেষ্টাই করে তার কমান্ডগুলো ঢুকানোর জন্য।আর ফোরাম,ব্লগের মাধ্যমে তা ছড়িয়ে দেই।

Tanbir Ahmad Razib
Mobile No:: 01738-359555//01916-457075//

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

T@NB!R 01738359555
E_Mail :: tanbir_cox@yahoo.com // tanbir.cox@gmail.com
Facebook:: http://www.facebook.com/tanbir.cox (srch: Tanbir Ahmad)

Web Site :: http://tanbir.99k.org

২.Mr.B

একজন হ্যাকার।তারও A এরমত ব্লগ আর ফোরাম আছে।সে বিভিন্ন প্রতিষ্ঠান আর ব্যক্তির গুরুত্বপূর্ণ ডাটা সংগ্রহের কাজে ব্যস্ত।এজন্য সে দরকারী প্রোগ্রাম তৈরি করে অনলাইনে ছেড়ে দেয় এবং বিভিন্ন লিংক এর সাথে যুক্ত করে দেয় যেখানে ক্লিক করলে প্রোগ্রামটি পিসিতে সেট হয়ে যায়।তার কাছে অসংখ্য মেইল এড্রেস আছে।সে নানা রকম অফার বা লোভ দেখিয়ে ঐ সব মেইল এড্রেসে মেইল পাঠায়(হয়ত যুক্তরাষ্ট্রের গ্রিন কার্ড বা লক্ষ ডলার লটারির অফার আপনিও পেয়েছেন যেখানে আপনার ক্রেডিট কার্ডের নংটা নির্ভুলভাবে বসাতে বলে)এমনকি আপনার বন্ধুর আইডি দিয়েও আপনাক মেইল পাঠায় যেখানে ছবি বা অন্য কিছুর কথা বলা থাকে অথচ আপনার অজান্তে তার প্রোগ্রামের লিংক যুক্ত করে দেয়।এতে মেইলটিতে ক্লিক করলে প্রোগ্রামটি পিসিতে যুক্ত হয়।।আর পিসির গুরুত্বপূর্ণ ডাটাগুলো

T@NB!R 01738359555
তার কাছে চলে যায় বা পিসিটিকে সে নিয়ন্ত্রণ করতে পারে।এভাবে সে বিভিন্ন প্রতিষ্ঠান ও ব্যক্তির ডাটা সংগ্রহ করে। আবার সে নাম করা বিভিন্ন প্রতিষ্ঠানের জন্য এমন প্রোগ্রাম তৈরি করে যেটা সব সময় ঐ প্রতিষ্ঠানের প্রতি নজর রাখে এবং ডাটা সংগ্রহ করার চেষ্টা করে।তাই আমরা অনেক সময় শুনে থাকি অমুক সাইটটি হ্যাক হয়েছে,অমুক প্রতিষ্ঠানে হ্যাকাররা হামলা চালিয়েছে বা কারো একাউন্ট শূণ্য হয়ে গেছে।আমরা এসব প্রোগ্রামকে সাধারণত মেইলওয়ার বা স্পাইওয়ার বলে চিনি।

উদাহরণ দিতে পারিঃ*সম্প্রতি ইউরোপের একটি দেশের প্রেসিডেন্টের ওয়েব সাইট হ্যাক হয়েছে।এতে তার ছবির বদলে হ্যাকাররা বিখ্যাত কৌতুক অভিনেতা মি:বিনের ছবি বসিয়ে দিয়েছে।ওয়েবসাইটটি খুললেই মি:বিন সবাইকে হাত নাড়িয়ে তার মুখের সুন্দর ভঙ্গি(সুন্দর ভঙ্গিটাতো বুঝতেই পারছেন)দিয়ে অভিবাদন জানাচ্ছে।*সম্প্রতি জনপ্রিয় সামাজিক যোগাযোগের সাইট টুইটার ইরানের হ্যাকাররা ৩ ঘন্টারও বেশি নিজেদের নিয়ন্ত্রনে রাখে।ততক্ষণে কর্তৃপক্ষ একবারও সাইটটিতে শত চেষ্টা করে ঢুকতে পারেনি।এখন তারা হাজার হাজার ইউজারের দুর্বল পাসওয়ার্ডগুলো বন্ধ করে দেওয়ার সিদ্ধান্ত নিয়েছে যেখানে বিখ্যাত নামি দামি ব্যক্তি,প্রতিষ্ঠানের পাসওয়ার্ডও রয়েছে।*আর চীনের ব্যাপারে গুগলের সিদ্ধান্তের কথাতো সবাই জানেন।*গতবছরের দিকে চীনের সেনাবাহিনী পেন্টাগণে হামলা চালায়।পেন্টাগণ দাবি করে তারা

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

প্রতিঘন্টায় একবার করে তাদের ডাটাগুলো স্ক্যান করে এবং সর্বক্ষণ নজরে রাখে।আর এরই ভিতর সল্পসময়েই চীনের সামরিক বাহিনী হামলাটি চালায়।তবে চীনের সেনাবাহিনী অভিযোকটি অস্বীকার করেছিল।*২০০৮ এর দিকে ব্রিটেনে এক হ্যাকারকে ১২ বছরের জেল দেওয়া হয় ক্রেডিট কার্ড হ্যাক করার দায়ে।সে স্বীকার করেছিল ২০০৪-২০০৬ এর ভিতর প্রায় ১০০ জনের ক্রেডিট কার্ড সে হ্যাক করেছিল।তবে সে কখনো ঐ সব একাউন্ট থেকে একবারে অর্ধেকের বেশি টাকা তুলেনি।এরকম অসংখ্য ঘটনা অনলাইনে নিয়মিত ঘটে যা সবসময় মিডিয়াতে আসেনা বা আসলেও আমরা পাইনা।

উপরে বর্ণিত A&B দুজনই কিন্তু খুবই দক্ষ প্রোগ্রামার।তারা বিভিন্ন ইন্টারনেট সিকিউরিটি ও এন্টিভাইরাসের ডেফিনিশনগুলো বিশ্লেষন করে দেখেই তাদের প্রোগ্রামগুলো তৈরি করে যেন যতটুকু সম্ভব এদেরকে ফাঁকি দেওয়া যায়।তাছাড়া তাদের বিরুদ্ধে অনলাইনে কি কি আলোচনা হয় তারা এ ব্যাপারেও সজাগ।প্রায় এক তৃতীয়াংশ বা তারও বেশি সাইট তারা নিয়ন্ত্রণ করে থাকে এবং তাদের সংখ্যা অনেক।হয়ত আমরা গুরুত্বপূর্ণ ব্যাক্তি নয় বলে B দের হামলাটা বুঝতে পারিনা।কিন্তু A দের জ্বালায় অতিষ্ট হচ্ছি নিয়মিত।

এভাবে A&B দের সাথে যুক্ত হয়ে পিস আক্রান্ত হয়।পরবর্তীতে ঐ ইউজার নিজেকে অন্যের সাথে শেয়ার করে।এভাবে ১ জন থেকে ৫জন১০জন হয়ে সংখ্যা বাড়ছেই।কেউ হয়তো বলতে পারেন আমি নেট ইউজ করিনা

T@NB!R 01738359555
কিন্তু আক্রান্ত হচ্ছি কেন।নেট ইউজ না করলেও আপনি পেনড্রাইভ ইউজ করেন বা বাজার থেকে সফটওয়ার সংগ্রহ করেন।কোনটাতে A&B দের হাত নেই আপনিতো জানেনা। তাহলে সিদ্ধান্ত নিতে পারি কম্পিউটার আক্রান্ত হয় ১.পেনড্রাইভ,সিডি - ডিভিডির মাধ্যমে ২.A&B এর লিংক ভিজিট করলে ৩.ভাইরাস এফেক্টেড ফাইল ইন্সটল করলে।৪.আপনার পিসি এমন একটি পিসির সাথে নেটওয়ার্কিং আছে যেটা ভাইরাসে আক্রান্ত।তাহলে ডাটা ট্রান্সফারের মাধ্যমে আপনার পিসিও ঐ ভাইরাসে আক্রান্ত হতে পারে।

৩.কি ভাবে কাজ করে:

কিভাবে কাজ করে তা জেনে লাভ নেই বরং তা একজন ইউজারের কী কী সমস্যা তৈরি করে তা জেনে নিই। শুরুতেই ১টা কথা বলি,**ভাইরাস কিন্তু সবসময় exeএক্সটেনশনের হয় এবং আক্রমণও করে exe এক্সটেনশনের ফাইলকে।তাই ইমেজ,টেক্সট,মিউজিক ইত্যাদি কোন ফাইল স্ক্যান করা আপনার নিষ্প্রয়োজন**।সুতরাং আমরা শুধু exe ফাইলের কথাই বলব এখানে।অন্যকোন ফাইলকে সে কখনো আক্রমণ করেনা।তাই exeছাড়া অন্য ফাইল কোন কারণে করাপ্টেড দেখলে ভাইরাসকে দায়ী করবেন না।বরং যেকোন ফাইল অপারেটিংগত ত্রুটির কারণে করাপ্টেড হতেই পারে।এবার আসুন সমস্যাগুলো দেখি।

১.একজন Administrative User কম্পিউটারকে নিজের মত চালানোর জন্য কিছু গুরুত্বপূর্ণ কমান্ড ব্যবহার

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

করে।যেমন:টাস্কমেনেজার(ctrl+alt+Delete)।বাকি গুলো হল cmd,msconfig,gpedit.msc,regedit কমান্ড যা Run এ গিয়ে দিতে দিতে হয়। বলতে গেলে এ কমান্ডগুলোতেই থাকে একজন Administrative User এর সর্বোচ্চ পাওয়ার।কিন্তু ভাইরাস এ কমান্ডগুলোকে ডিজেবল করে দেয়।শত চেষ্টা করলেও(থার্ডপার্টি সফটওয়ার ছাড়া)কমান্ডগুলো কাজ করেনা।

২.ফোল্ডার অপশন ডিজেবল হয়ে যায়।কখনো ফোল্ডার অপশন থাকে কিন্তু Show hidden files and folders অপশনটা কাজ করেনা।আপনি এই দিছেনতো অকে দেওয়ার পর আবার সেই আগের জায়গায় চলে যায়।

৩.কখনো দেখা যায় আপনার ইন্সটল করা প্রোগ্রামগুলো কিছুক্ষণ পর খুলছেনা।খুলতে গেলে মেসেজ দেয়exe ফাইলটি পাওয়া যাচ্ছেনা।ইন্সটল করা সব প্রোগ্রামই এ সমস্যা করবে তেমন নয় বরং যে কটাকে ধরেছে এগুলোই করে।সাধারণত ভাইরাস এফেক্টেড সফটওয়ার ইন্সটল করলেই এ সমস্যা হয়।

৪.উইন্ডোজ খোলার পথে বন্ধ হয়ে যায়,দাঁড়িয়ে থাকে বা বার বার রিস্টার্ট নেয়।

৫.আমরা যখন অফিস ডকুমেন্টের(ওয়ার্ড,এক্সেল ইত্যাদি)কাজ করি তখন এগুলোর টেম্প ফাইল তৈরি হয় এবং ফাইল ক্লোজ করলে এগুলো অটোমেটিক চলে

T@NB!R 01738359555
যায়।কিন্তু ভাইরাস এফেক্টেডের কারণে এগুলো যায়না বরং জমা হতে থাকে।

৬.পিসিতে পেনড্রাইভ দিলেই অটোরান সহ অপরিচিত ফাইল তৈরি হয়।তাছাড়া পেনড্রাইভকে Safly remove করতে গেলে সেফলি রিমোভ হবেনা মেসেজ দেয় অর্থাৎ পেনড্রাইভকে Safly remove করা যায়না।

৭.EXPLORER.EXE এর Process বন্ধ হয়ে যায় যার ফলে ডেস্কটপের সবকিছু অদৃশ্য হয়ে যায়।
আরো কিছু উপসর্গ মাঝে মধ্যে দেখা যায়।তবে উপরের কারণগুলো যদি দেখেন তাহলে আপনি নিশ্চিত হতে পারেন আপনার পিসিটি ভাইরাস আক্রান্ত।সবগুলো উপসর্গই যে একসাথে পাবেন তেমন কিন্তু নই।বরং একটা দুটা যেকটা পাবেন তাই।উপরুক্ত চিহ্নগুলো চেক করে(বিশেষ করে ফোল্ডার অপশন আর পেনড্রাইভ সমস্যা) কোন পিসিতে হাত দিয়ে আপনি মুহূর্তেই বলে দিতে পারবেন ঐ পিসিটি ভাইরাস আক্রান্ত কিনা।
এবার বলি **আপনার পিসির কী কী ক্ষতি করতে পারে**।মূলত উপরে বর্ণিত কাজগুলো দ্বারা সে আপনার উইন্ডোজকে নিজের নিয়ন্তণে নেয়।আপনার পিসিতে দিনের পর দিন ঐ সমস্যাগুলো একটা থেকে দুটা বাড়তে থাকে।আস্তে আস্তে সি ড্রাইভ(উইন্ডোজ ড্রাইভ)থেকে চলে যায় অন্য ড্রাইভে।১মে অন্য ড্রাইভের System Volume Information কে আক্রমণ করে।পরে ঐড্রাইভে যেexe ফাইল বা সেটআপ ফাইল থাকে তাকে

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

TANBIR 01738359555
আক্রমণ করে।ফলে আক্রান্ত ফাইলটা হয়ে যায় ভাইরাস এফেক্টেড ফাইল।পরবর্তীতে আপনি সেটা ইন্সটল করেন।অথচ সে ফাইলগুলো আপনার মুল্যবান বেকআপ ফাইল।তাছাড়া কোন কোন ভাইরাস ড্রাইভগুলোতে অটোরান ফাইল তৈরি করে।এঅবস্থায় ডাবল ক্লিক করলে ড্রাইভগুলো খোলেনা বরং এক্সপ্লোরার থেকে খুলতে হয়।অটোরান ফাইলটি মুছে দিলেও পরে আবার তৈরি হয়।কারণ আপনার উইন্ডোজটা আক্রান্ত।

সম্ভব হলে একটা পরামর্শ নিন:-

আপনার পিসি যখন ভাইরাসে আক্রান্ত হয় তখন উপরের সমস্যাগুলো কিছু থার্ডপার্টি সফটওয়ার দিয়ে সাময়িক নিরাময় করা যায়।কিন্তু জরুরি প্রয়োজনটা মিটিয়েই সচেতন হোন।তখন ওইন্ডোজটা রিইন্সটল না দিয়ে পুরু দেবেন।কেন দেবেন?থার্ডপার্টি দিয়ে সমাধান পেয়েছেন মানে এ নয় আপনি ভাইরাসটা শেষ করতে পেরেছেন।বরং সেটা তার কাজ চালিয়ে যায় যতক্ষণ পিসি ওপেন থাকে।আপনি বলতে পারেন এন্টিভাইরাস দিয়ে স্ক্যান করব আর কি।একদম শুরুর পর্যায়ে হলে আপনার কথাটা ঠিক আছে।কিন্তু ভাইরাসটা খুব শক্তিশালি হলে বা বেশি ছড়িয়ে পড়লে আপনার কথাটার কোন মুল্য নাই।তাছাড়া ভাইরাস সিস্টেম ফাইলগুলোকে খুবই দুর্বল করে ফেলে। তাই আপনি স্ক্যান করে ভাইরাসগুলো তাড়াতে পারলেও আক্রান্ত সিস্টেম ফাইলগুলো পুরো

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

পারফরমেন্স দেখাতে পারেনা।তখন পিসি হয়ে যায় স্লো।তাছাড়া শক্তিশালি ভাইরাসগুলো এন্টিভাইরাসকে ফাঁকি দিয়ে একবার ঢুকতে পারলে এন্টিভাইরাস তাকে আর ধরতে পারেনা।কিন্তু কষ্ট করে বিলগেটসকে নতুনভাবে দিয়ে দিলে ঝামেলা শেষ।তখন ড্রাইভের অটোরান ফাইলগুলোও ডিলিট করতে পারবেন সহজে।তবে অবশ্যই এ সমস্যায় ড্রপডাউন মেন্যু দিয়ে ড্রাইভে ঢুকবেন।

৪.কিভাবে দূর করা যায়ঃ

উপরের লেখাগুলো পড়লে আপনার অবশ্যই ১টা ধারনা আসার কথা কিভাবে পিসি থেকে ভাইরাস দূর করা যায়।তাই আমি আগে আলোচনা করছি ভাইরাস থেকে বাঁচার উপায় কি।এই পর্যন্ত এন্টিভাইরাসকেই ভাইরাসের একমাত্র ঔষধ বলে সবাই স্বীকার করে।তবে আমি পুরোটা করিনা।কারণ আপনি নিজেই কিছু কাজ করতে পারেন।এন্টিভাইরাস দরকার শুধুমাত্র ভাইরাস এফেক্টেড ফাইল চেক করার জন্য।অরজিনাল ভেন্ডর ছাড়া অন্য কারো কাছ থেকে সংগ্রহ করা সফটওয়ারগুলো কিন্তু ১০০% নিরাপদ নয়।আর আমরা কোন্ কালে অরজিনাল ভেন্ডর থেকে সফটওয়ার সংগ্রহ করেছি?তাই আমাদের সংগ্রহ করা সফটওয়ারগুলো ভাইরাস এফেক্টেড কিনা তা চেক করার জন্য এন্টিভাইরাসই একমাত্র ভরসা।তাছাড়া A&B এর হাত থেকে বাঁচার জন্য

T@NB!R 01738359555
এন্টিভাইরাস আর ইন্টারনেট সিকিউরিটি ছাড়া তেমন কোন নিরাপদ ব্যবস্থা নেই।তবে দুঃখের বিষয় হল এগুলোর কোনটাই আপনাকে ১০০% নিরাপত্তা দিতে পারবে এমন গ্যারান্টি কেউ দিতে পারবেনা।আপনি এগুলোর মাধ্যমে সর্বোচ্চ ৮০থেকে৯০ভাগ নিরাপত্তা পেতে পারেন তা যে ব্রান্ডেরই মাল হোক না কেন।এর বিনিময়ে তাকে দিতে হবে মিনিমাম ৫০ মে:বা: জায়গা,প্রতি সপ্তাহে আপডেটের সুযোগ,কম্পিউটারকে স্লো করার অধিকার।কখনো আপনার সুস্থ কোন ফাইলকে অসুস্থ বলেও ধরবে কিন্তু।সে অপমানও আপনাকে সইতে হবে।আর লাইসেন্সের ঝামেলাতো রয়েছে।চুরি করে কদিনই বা চলে?ঐ যে স্কুলে পড়েছিলামনা পেট শুধু খাই আর খাই,কোন কাজ করেনা।এন্টিভাইরাস আর কি।এত ঝামেলার পরেই নিরাপত্তা পেতে পারেন।তাই আমি এগুলো নিয়মিত ব্যবহারের পক্ষে নয়।আমি সফটওয়ার সংগ্রহ করতে করতে অনেকগুলো হলে তখন এগুলোকে একবার যে কোন দুটা(না পারলে অন্তত১টা) এন্টিভাইরাস দিয়ে স্ক্যান করিয়ে নিই।তারপর সিডিতে রাইট।আর এভাবে আমি খুব নিরাপদেই থাকতে পেরেছি এ পর্যন্ত। যাক এবার ১ম থেকে কাজগুলো শুরু করুন পর্যায়ক্রমে।নতুনভাবে উইন্ডোজ দিন।অটোরান বন্ধ করে দিন।তারপর সিস্টেম রিস্টোর বন্ধ (My Computer>Properties>System Restoreএ গিয়েTurn off System Restore on all drivesএর চেক তুলে দিয়েYes,Okকরে)পিসি রিস্টার্ট দিন।এবার সি সহ সমস্ত ড্রাইভের System Volume

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

T@NB!R 01738359555
Information_restore{9E42ABDF-336B-4093-AF0F-2F23508C78D5}এর ভিতরের সমস্ত ফাইল ডিলিট করে দিন।এর ফলে আপনি সিস্টেমকে রিস্টোর(যেটা আমারা খুব করি)করার সুযোগটা আর পাবেনা,বিনিময়ে ভাইরাস আপনার কম্পিউটারে স্থায়ী বাসা বাঁধতে পারবেনা,হার্ডডিস্কের অনেক জায়গা খালি হবে।বেকআপে থাকা আপনার সমস্ত সফটওয়ার ফাইলকে আপডেট এন্টিভাইরাস দ্বারা স্ক্যান করে নিন।এখন আপনি ভাইরাসমুক্ত।এবার আপনার স্ক্যান করা ফাইলগুলো থেকে যা যা আপনার দরকার ইন্সটল করে নিন।বেকআপ থাকা সন্দেহজনক সফটওয়ারগুলো ডিলিট করে দিন। আপনার পছন্দমত সেটিংসটা শেষ করে (লিংকটি দেখতে হলে অবশ্যই প্রবেশ অথবা নিবন্ধন করতে হবে)দিয়ে একটা ইমেজ তৈরি করে নিন যাতে ভবিষ্যতে উইন্ডোজ দিতে আর বিরক্তিবোধ না করেন।তাহলে যেকোন সফটওয়ার স্ক্যান না করেই ব্যবহার করতে পারবেন।যদি দেখেন ঐ সফটওয়ার ইন্সটল করার কারণে পিসি আক্রান্ত হয়েছে তাহলে হিরেনবুটস দিয়ে ৫ মিনিটের কাজটা সেরে নেবেন আর ধরে নেবেন সফটওয়ারটিA&Bএর মাল।তাহলে আপনিও আমার মত এন্

এন্টিভাইরাস সফটওয়্যার এবং - প্রতিরোধমূলক ব্যবস্থা অন্যান্য

দুটি সাধারণ পদ্ধতিতে এন্টি- ভাইরাস সফটওয়্যারগুলো ভাইরাস সনাক্ত করে থাকে। প্রথম ও সর্বাধিক প্রচলিত পদ্ধতিটি হল ভাইরাস সিগনেচার

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

T@NB!R 01738359555
সংগ্রহার তালিকা থেকে ভাইরাস সনাক্তকরণ। এই সনাক্তকরণ পদ্ধতির প্রধান সমস্যা হল ব্যবহারকারীরা কেবল সেসব ভাইরাস থেকেই রক্ষা পান যেগুলো পুর্বোক্ত ভাইরাস সংগ্রহার আপডেটে উল্লিখিত থাকে। দ্বিতীয় পদ্ধতিটি হল হিউরিস্টিক এলগরিদম যা ভাইরাসের সাধারণ সংগ্রহা থেকে সনাক্ত করা হয়। এই পদ্ধতিতে এন্টি- ভাইরাস সিগনেচার ফার্ম কর্তৃক সংগ্রহায়িত ভাইরাস না হয়েও তা সনাক্ত করা যায়।

সারানোর প্রক্রিয়া

কোন কম্পিউটার একবার ভাইরাস দ্বারা আক্রান্ত হবার পর অপারেটিং সিস্টেম পুনরায় ইনস্টল করা ছাড়া তা ব্যবহার করা বিপদজনক। তবে ভাইরাস আক্রান্ত কম্পিউটারকে সারিয়ে তোলার জন্য বেশ কয়েকটি পদ্ধতি রয়েছে। এই পদ্ধতিগুলো ভাইরাসের প্রকার ও আক্রান্ত হবার মাত্রার উপর নির্ভর করে।

ভাইরাস মুছে ফেলা

উইণ্ডোজ এক্স পিতে ক্ষতিগ্রস্ত সিস্টেমকে পূর্বাবস্থায় ফিরিয়ে নিয়ে আসার পদ্ধতিটি সিস্টেম রিস্টোর নামে পরিচিত, যা রেজিস্ট্রি এবং গুরুত্বপূর্ণ সিস্টেম ফাইলসমূহকে স্বাভাবিক অবস্থায় ফিরিয়ে নিয়ে আসে। অনেক সময় এর প্রয়োগ ভাইরাস সিস্টেমটিকে হ্যাং করে দেয় এবং পরবর্তীতে হার্ড রিবুট এটিকে ক্ষতিগ্রস্ত করার আগের অবস্থায় নিয়ে যাবে। অবশ্য কিছু ভাইরাস রিস্টোর সিস্টেমসহ অন্যান্য গুরুত্বপূর্ণ টুল যথা টাস্ক ম্যানেজার এবং কমাণ্ড প্রম্পট

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

T@NB!R 01738359555
বিকল করে দেয়। এগুলো করে এমন একটি ভাইরাসের নাম সায়াডোর। বিভিন্ন উদ্দেশ্যে এডমিনিস্ট্রেটরের উক্ত টুলগুলো অন্যান্য ব্যবহারকারীদের জন্য অকেজো করে রাখার ক্ষমতা আছে। ভাইরাস রেজিস্ট্রিকে পরিবর্তন করে দেবার মাধ্যমে একই কাজ করে, ফলে যখন একজন প্রশাসক কম্পিউটারটি চালান তখন তিনিসহ অন্যান্য ব্যবহারকারী এই টুলগুলো ব্যবহার করা থেকে বঞ্চিত হন। যখন একটি আক্রান্ত টুল ভাইরাসের মাধ্যমে অকেজো হয়ে যায় তখন তা "Task Manager has been disabled by your administrator." বার্তাটি দেয়।

অপারেটিং সিস্টেমের রিইন্সটলেশন

যদি কোন কম্পিউটারে এমন কোন ভাইরাস থাকে যা এন্টি ভাইরাস সফটওয়্যারের পক্ষে মুছে ফেলা সম্ভব না হয় তবে অপারেটিং সিস্টেমের পুনরায় ইন্সটলেশন জরুরি হতে পারে। এটি সঠিকভাবে করার জন্য হার্ড ড্রাইভ সম্পুর্ণভাবে ডিলিট করতে হবে (পার্টিশন ডিলিট করে ফরম্যাট করতে হবে)।

সর্তকতা

কম্পিউটারকে ভাইরাসের আক্রমণ হতে রক্ষা করার জন্য সর্তকতার কোন বিকল্প নেই। আগে আমরা দেখি ভাইরাস ছড়ায় কেমন করে। কোন ভাইরাজই নিজ থেকে সক্রিয় হতে পারে না, ভাইরাস প্রোগ্রাম সক্রিয় হবার জন্য বিভিন্ন কৌশল ব্যবহার করে এবং আমরা এই সকল ভাইরাসের ধোকায় পরে নিজেদের অজানতেই ভাইরাস প্রগ্রামকে সক্রিয়

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

T@NB!R 01738359555
করে ফেলি।ভাইরাজ বা ওয়ার্ম প্রগ্রাম ফাইল শেয়ারিং অথবা পেন ড্রাইভের মাধ্যমে ছড়ায় যা আমরা হয়তো অনেকেই দেখেছি। ভাইরাস আক্রান্ত পিসিতে পেনড্রাইভ লাগালে ভাইরাসটি পেনড্রাইভে তার একটা কপি তৈরি করে। আর একটা autorun.inf ফাইল তৈরি করে দেয়। এই আক্রান্ত পেনড্রাইভটি অন্য পিসিতে লাগানোর পর এর সাথে জড়িত যেকোন "Event" ঘটলে (যেমন open বা explore করলে) autorun.inf ফাইলটি সক্রিয় হয়ে ভাইরাসটিকে Execute করে দেয়। যেমন: কম্পিউটারে পেন ড্রাইভ যুক্ত করলে Autoplay প্রম্পটে আসবে এবং এখান থেকে open বা explore যে অপশনটিই নির্বাচন করি না কেন autorun.inf ফাইলটি সক্রিয় হয়ে ভাইরাসটিকে Execute করে দিবে।তার মানে কোনভাবে এই autorun.inf ফাইলকে তৈরি হতে দেয়া না হলে, ভাইরাস পেনড্রাইভে থাকলেও Execute করবে না।

এখন সমাধান হল আগে থেকে আপনি আপনার পেনড্রাইভে একটা autorun.inf নামে "ফোল্ডার" (ফাইল নয়) তৈরি করে রাখুন। তাহলেই তাকে রিপ্লেস করে আক্রান্ত পিসির ভাইরাসটি নিজস্ব autorun.inf ফাইল তৈরি করতে পারবে না। কারণ, বেশিরভাগ ভাইরাস নির্মাতারা এই বিদঘুটে সমভাবনাটা এড়িয়েই যান।

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

অথবা কম্পিউটারকে ভাইরাসের আক্রমণ হতে রক্ষা করার জন্য নিচের কৌশলটিও ব্যবহার করা যেতে পারে।

- পেন ড্রাইভ লাগালে Autoplay প্রম্পট আসবে , এই Autoplay প্রম্পটকে বন্ধ করতে হবে এবং লক্ষ্য রাখতে হবে এই Autoplay প্রম্পটের কোন অপশন যেনো নির্বাচন করা না হয় করণ বেশির ভাগ ক্ষত্রেই ভাইরাজ প্রগ্রাম সক্রিয় হবার জন্য “Windows Explorer” ব্যবহার করে। এই অপশনটি উইন্ডোজ এর ডিফল্ট অপশন, যা ব্যবহার করে আমারা উইন্ডোজের বিভিন্ন ধরনের কাজে ব্যবহার করে খাকি। সেই সুযোগেই এই সকল ক্ষতিকর প্রোগ্রাম আমাদের কম্পিউটারের ক্ষতি করার সুযোগ পায়। আমরা নতুন পেন ড্রাইভ কম্পিউটারে লাগিয়ে পেন ড্রাইভ খোলার জন্য “Windows Explorer” ব্যবহার না করে অন্য কোন “Explorer” ব্যবহার করি তবে এই সকল ক্ষতিকর প্রোগ্রাম আমাদের কম্পউটারের ক্ষতি করার সুযোগ পাবে না।

অতিরিক্ত “Explorer” হিসাবে “Win Rar” বেশ ভালো কাজ করে। মনে করুন আপনি আপনার কম্পিউটারে একটি পেন ড্রাইভ ব্যবহার করার জন্য লাগিয়েছেন এখন Autoplay প্রম্পট আসেছে। আপনি সর্তকতার জন্য Autoplay প্রম্পটকে বন্ধ করে দিয়েছেন কিন্তু আপনার পেন ড্রাইভ খুলতে হবে। সে ক্ষত্রে “Win Rar” ওপেন করে Address Bar থেকে Drive Letter (যেমনঃ D:\ বা I:\) টাইপ করে এন্টার দিন ব্যাস আপনার

পেন ড্রাইভের ডাইরেক্টরি খুলে যাবে এখন এই ডাইরেক্টরি থেকে প্রয়োজনীয় ফাইলটি নির্বচন করে এন্টার দিলেই ফাইলটি ওপেন হয়ে যাবে। যে পযন্ত আপনি না চাইবেন সে পযন্ত কোন ফাইল বা প্রোগ্রাম নিজ থেকে চালু হবে না।

সবসময় সিস্টেম ফাইল Show করুন

ভাইরাসের এক্সিকিউটেবল (*.exe) ফাইলগুলোর Attibute হয় সাধারণত Hidden এবং System File যা সাধারণত Show করা থাকে না। তাই আপনি বুঝতেও পারেননা আপনার পেনড্রাইভে ভাইরাস আছে কিনা। এধরনের ফাইল চিহ্নিত করতে Tools মেনু থেকে Folder Options এ গিয়ে View ট্যাব থেকে Show Hidden Files and Folders রেডিও বাটন সিলেক্ট করুন।এবার ঠিক তার নিচের Hide Extensions for known File Types এবং Hide Protected Operating System Files লেখা দুটি চেকবক্স আনচেক করে Apply দিয়ে Ok করে বেরিয়ে আসুন। এবারে পেনড্রাইভে সন্দেহজনক কোন Hidden এক্সিকিউটেবল (*.exe) ফাইল দেখলে ডিলিট করে দিন।

Drive Letter টাইপ করে পেনড্রাইভ খুলুন

ভাইরাস আক্রান্ত বা সন্দেহজনক পেনড্রাইভ কখনোই ডাবলক্লিক করে অথবা রাইট বাটনে ক্লিক দিয়ে (Open বা Explore করে) খুলবেন না। Address Bar থেকে Drive Letter (যেমনঃ D:\ বা I:\) টাইপ করে খুলবেন। এতে ভাইরাস থাকলেও তা

আপনার পিসিকে আক্রান্ত করার সুযোগ পাবে না। একইভাবে হার্ডডিস্কের অন্যান্য পার্টিশনে ভাইরাস থাকলে তা ডিলিট করুন এবং পিসি রিস্টার্ট দিন।

স্টার্টআপ পরিষ্কার রাখুন

আপনার পিসি Boot করার পর যেসব প্রোগ্রাম লোড করে তা থাকে স্টার্টআপে। নিত্যপ্রয়োজনীয় প্রোগ্রামগুলো ছাড়া অন্যান্য প্রোগ্রামগুলোর চেকবক্স আনচেক করে দিন। এটি আপনি পাবেন উইন্ডোজের Run থেকে msconfig লিখে এন্টার দিলে যে ডায়ালগ বক্স আসবে তার Startup ট্যাব থেকে। এবারে পিসি রিস্টার্ট দিন।

অপ্রয়োজনীয় Process দূর করুন

অনেকসময় ভাইরাস ফাইল চিহ্নিত করার পরেও তা ডিলিট করতে গেলে এরর দেয় বা “Access is Denied” দেখায়। এরকম হলে বুঝতে হবে ভাইরাস Process টি বর্তমানে Running অবস্থায় আছে যা আগে বন্ধ করতে হবে। আপনি Ctrl+Alt+Delete চেপে Task Manager থেকে প্রসেসটি বন্ধ করতে পারেন। কিন্তু সমস্যা হয় তখনই যখন প্রসেসটি থাকে Hidden যা Task Manager এ Show করে না। এক্ষেত্রে আপনি HijackThis নামের সফটওয়্যারটি ব্যবহার করতে পারেন যা বেশ ভাল একটি Spyware Remover।

Spyware:Which is a such kind of malware>এটা আপনার পিসি

থেকে তথ্য নিয়া অন্য কোন ব্যক্তির(যে এটি পাঠিয়েছে) কাছে দিবে এতে করে আপনার অনেক প্রয়োজনিয় তথ্য অন্য কেউ জেনে যাবে এতে কেমন ক্ষতি হবে তা আর বলার অপেক্ষা রাখেনা।

কিভাবে কম্পিউটারকে রাখবেন পুরোপুরি ভাইরাস মূক্ত

Virus,আমরা যারা কম্পিউটার ব্যবহার করি,তারা সবাই এই শব্দটার সাথে পরিচিত,কারন এটি আমাদের সবার একটি common সমস্যা।এর থেকে পরিত্রানের জন্য আমরা বিভিন্ন রকম এন্টিভাইরাস ব্যবহার করি।কিন্তু সমস্যা হচ্ছে,

১)কোনো এন্টিভাইরাস ই সব ভাইরাস ডিলিট করতে সক্ষম নয়,তা যত ভাল এন্টি ভাইরাস হোক না কেন,কারন কোনো এন্টি ভাইরাসেই সব ভাইরাস ডেফিনিশন দেয়া থাকে না।

২)এন্টিভাইরাস ইন্সটল করার পরে তা র‍্যাম এর কিছু জায়গা দখল করে।তাই ভারি এন্টিভাইরাসের ক্ষেত্রে র‍্যাম এ ব্যবহার করা জায়গার পরিমানও বেশি।ফলে কম্পিউটার স্লো হতে পারে।

সুতরাং,করণীয় কি?হ্যা বন্ধুরা,আমি আমার এই পোষ্টে এই সমস্যার সমাধানের ব্যাপারে লিখলাম।আশা করি,উপকৃত হবেন।

আসুন প্রথমেই জেনে নিই ভাইরাস কি?এটি কোনো বায়োলজিক্যাল ভাইরাস নয়।বরং এটি এমন একটি

প্রোগ্রাম যা কম্পিউটারের স্বাভাবিক কার্যকলাপকে বিঘ্নিত করে।এমনকি সিস্টেমের মারাত্বক ক্ষতিও হতে পারে(উদাহরনস্বরূপ,কম্পিউটার স্লো হয়ে যাওয়া,অকারণে রিষ্টার্ট নেয়া,টাস্ক ম্যানেজার ডিজেবল হওয়া ইত্যাদসহ আরো অনেক কিছু)

এবার আসুন জেনে নিই ভাইরাস কীভাবে কম্পিউটারে প্রবেশ করে।

১)পেনড্রাইভ,ডিস্ক,মেমরী কার্ড বা অন্য যেকোনো এক্সটারনাল ডিভাইসের মাধ্যমেঃ ভাইরাস আছে,এমন ডিভাইস কম্পিউটারে কানেকশান পাওয়ার পরে যখন আপনি তা ওপেন করবেন,তখন।

২)ইন্টারনেট থেকেঃযখন আপনি ভাইরাস আছে,এমন কোনো সাইটে প্রবেশ করবেন।

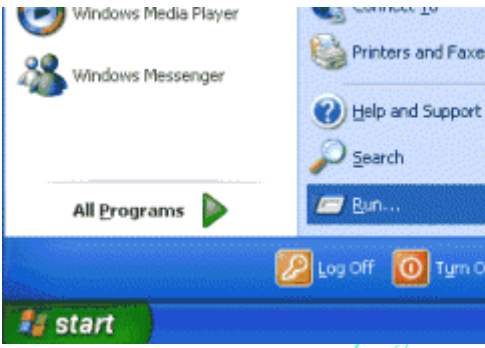
চলুন এবার জেনে নিই এক্সটারনাল ডিভাইসের ভাইরাস থেকে কিভাবে পিসি কে মুক্ত রাখতে পারি।আপনাদের জন্য ধাপে ধাপে নিচে বিষয়টি উপস্থাপন করা হল।

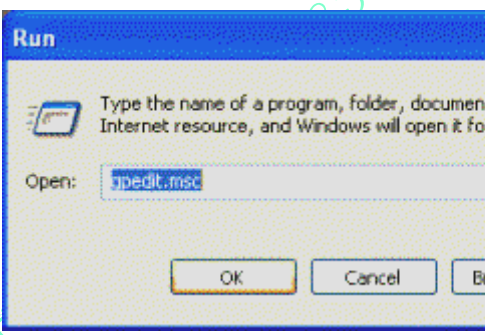
১)যেহেতু,ভাইরাস ইনফেক্টেড এক্সটারনাল ডিভাইস(যেমন পেনড্রাইভ)ওপেন করার পরেই ভাইরাস পিসিতে প্রবেশ করে,তাই এগুলো পিসিতে কানেকশান দেয়ার পরে তা ওপেন করা থেকে বিরত থাকতে হবে।ভাবছেন,তাহলে ডাটা ট্রান্সফার করবেন কীভাবে?এই ব্যাপারে একটু পরেই বলবো।

২)কখনো কখনো এক্সটারনাল ডিভাইস পিসিতে কানেকশান পাওয়ার

সাথে সাথে তা নিজে থেকেই ওপেন হয়।ফলে,ভাইরাস পিসিতে প্রবেশ করে ফেলে।তাই,ডিভাইস যেনো অটোম্যাটিকেলী ওপেন না হয় তাই নিচের পন্থা অনুসরন করতে পারেন।

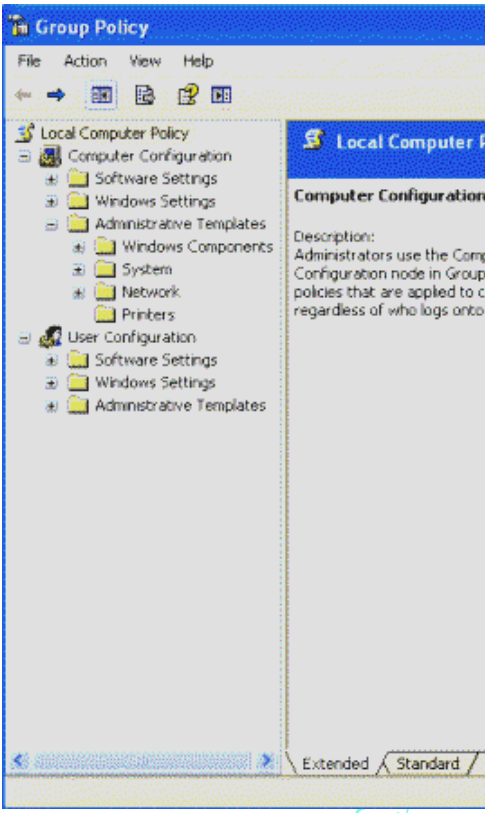
ক) start থেকে run এ গিয়ে টাইপ করুন, gpedit.msc । এরপর ok বাটনে ক্লিক করুন।





খ) এর ফলে নিচের মত একটি উইন্ডো দেখতে পাবেন।এই উইন্ডো থেকে computer configuration সিলেক্ট করুন।

T@NB!R 01738359555

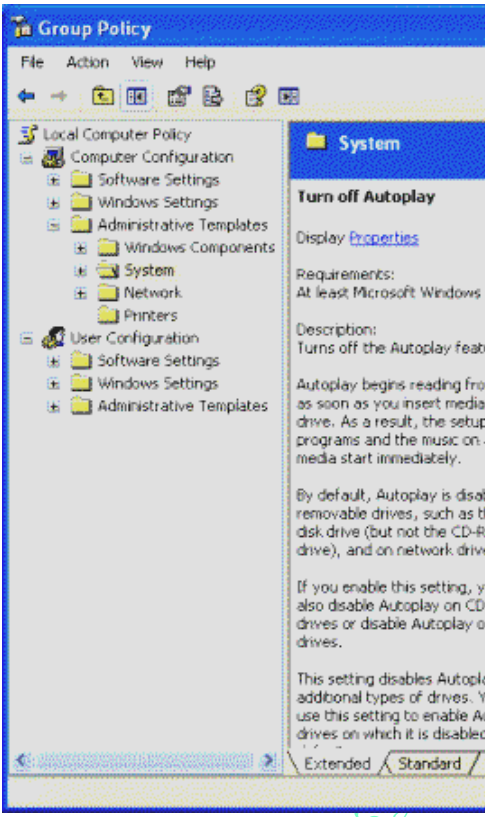


গ)এখান থেকে administrative tamplates->system এ যান।এখানে নিচের মত উইন্ডো পাবেন।এখান থেকে turn off autoplay তে ডাবল ক্লিক করুন।

T@NB!R 01738359555

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

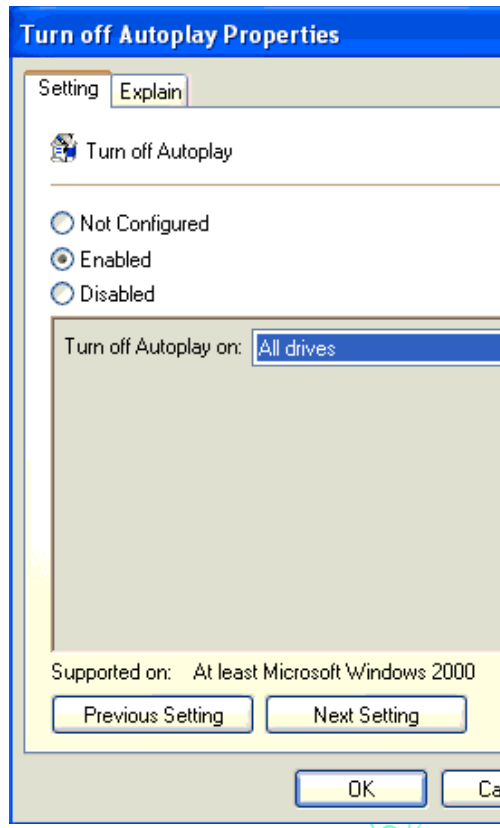
T@NB!R 01738359555



ঘ)নিচের মত উইন্ডো পাবেন।এখান থেকে “turn off autoplay” enable করুন এবং এর নিচে লেখা “turn off autoplay on” ড্রপ-ডাউন বক্স থেকে “All drives” সিলেক্ট করুন,এরপর ok বাটনে ক্লিক করুন।

T@NB!R 01738359555

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

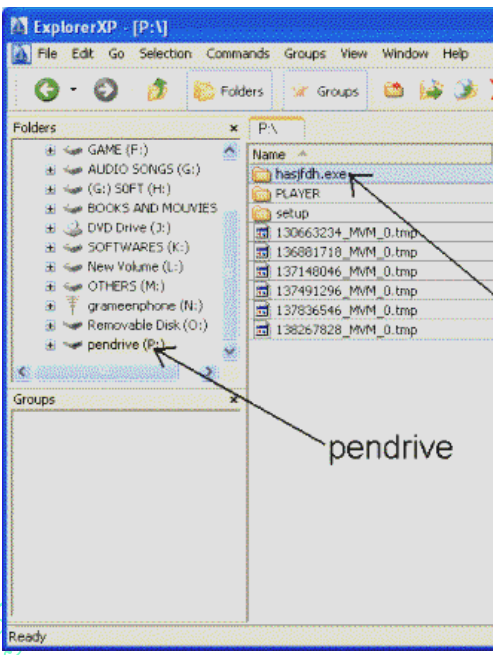


এখন কোনো পেনড্রাইভ পিসিতে প্রবেশ করালেও তা আর নিজে থেকে খুলবে না।

২)এখন ডাটা ট্রান্সফার করবেন কীভাবে?এর জন্য আপনাকে এমন কিছু করতে হবে যেনো,পেনড্রাইভ বা অন্য যে কোনো ডিভাইস যা আপনি পিসিতে লাগিয়েছেন তা যেনো না খুলেই তা থেকে ডাটা নিতে পারেন।এজন্য আপনাকে ছোট্ট একটি সফটওয়্যার ইন্সটল করতে হবে।ভয় পাবেন না।এর সাইজ মাত্র ৪১০ কিলোবাইট।ডাউনলোড করুন এখান থেকে।

সফটয়্যারটি ইন্সটল করার পরে রান করলে নিচের মত উইন্ডো পাবেন যার বামপাশে আপনার পিসির সব ড্রাইভগুলো দেখা যাবে।যেকোনো ড্রাইভে ক্লিক করলে এর ডানপাশে ঐ ড্রাইভের কন্টেন্ট দেখতে পাবেন।এখন

বামপাশ থেকে পেনড্রাইভটি সিলেক্ট করলে ডানে এর ডাটা দেখতে পাবেন।যদি এতে ভাইরাস থাকে,তবে তাও দেখতে পাবেন(এমনকি hidden ফাইলও)।এখান থেকে আপনি আপনার প্রয়োজনীয় ফাইলগুলো নিয়ে নিন,আর পেনড্রাইভের ভাইরাসকে পেনড্রাইভেই রেখে দিন।(উল্লেখ্য,কোনো ফোল্ডারের নামের সাথে .exe এক্সটেনশান থাকলে তা অবশ্যই ভাইরাস,এগুলো কপি করা থেকে বিরত থাকুন।)



লক্ষ্য করুন উপরে বামে পেনড্রাইভে ক্লিক করার ফলে ডানপাশে এর কন্টেন্টগুলো দেখা যাচ্ছে।এগুলোর মধ্যে .exe এক্সটেনশানযুক্ত একটি ফোল্ডার(hasjfdh.exe) আছে।এটি একটি ভাইরাস।

৩)যারা ভাইরাস সনাক্ত করতে পারেন না,তারা এমন কোনো থিম ব্যবহার করতে পারেন যা ফোল্ডারের কালার বা চেহারা/আইকন change করে,ফলে আপনার পেনড্রাইভের এবং পিসির ফোল্ডারের কালার বা চেহারা/আইকন

T@NB!R 01738359555
change হবে(উদাহরনস্বরূপ,আপনি universal vista inspirat Brico Pack Ultimate 2 1.0 ব্যবহার করতে পারেন।ডাউনলোড করুন এখান থেকে।)কিন্তু যেসব ফোল্ডারের চেহারা/আইকন পরিবর্তিত হবে না,সেগুলোই হলো ভাইরাস,এছাড়াও পেনড্রাইভে অনাকাঙ্খিত বা উদ্ভট টাইপের কন্টেন্ট থাকলে সেগুলোও ভাইরাস হিসেবে আপনি ধরে নিতে পারেন।

৪)কাজ শেষে পেনড্রাইভটি খুলে ফেলুন ভাইরাসসহ অথবা যদি চান তবে ফরম্যাটও করে আপনার পিসির ডাটা এতে ট্রান্সফার করতে পারেন।

উপরোল্লিখিত উপায়ে আপনি ভাইরাস থেকে পিসিকে মুক্ত রাখলেও আপনার পিসিতে যদি আগে থেকেই ভাইরাস থাকে সেক্ষেত্রে কি করবেন?তার জন্য আপনি কয়েকটি এন্টিভাইরাস দিয়ে স্ক্যান করে(যেহেতু একটা এন্টিভাইরাস সব ভাইরাস নাও ধরতে পারে) নিশ্চিত করুন যে,আপনার পিসিতে আর কোনো ভাইরাস নেই।তারপর উপরের পদ্ধতি apply করতে পারেন।

যদি এমন হয় যে,আপনার পিসিতে আগে থেকেই ভাইরাস ছিলো এবং এর ফলে আপনি এন্টিভাইরাস ইন্সটলই করতে পারছেন না,তাহলে আপনি স্ক্যান করবেন কিভাবে?আপনি হয়তো বলবেন এক্সপি সেটআপ দিলেই সব ঠিক হবে।কিন্তু ভাইরাস যদি সিস্টেম ড্রাইভে না থেকে অন্য ড্রাইভে থাকে তবে ত এক্সপি সেটআপে কাজ হবে না,কারণ এতে শুধু সিস্টেম ড্রাইভই ফরম্যাট হবে,অন্য ড্রাইভের ভাইরাস অন্য ড্রাইভেই থাকবে।

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

TANBIR 01738359555

ভাইরাস!!!

পৃথিবীর প্রথম কম্পিউটার ভাইরাসের নাম কি?

আমি জানিনা। শেষ। কোন চান্সই নাই আমার পরিক্ষায় পাশ করার। আপনারা জানলে নিচে মন্তব্যের স্থানে উত্তরটা দিয়ে দিবেন। আমি আমার বড় ভাইটাকে জানায় দিবো। উনি রিটার্ন টেষ্টে এই প্রশ্নের উত্তর দিয়ে এসেছেন "none of those"। মানে আরও তিনটা ছিলো উত্তর, উনার মনে হয়েছে এর কোনটাই নয়। হতেই পারে এমন। তাছাড়া ওখানে যদি সঠিক উত্তরটি থেকেও থাকে তা উনার জানার কথা না। আমরা কয়জন জানি! সেই ১৯৯৮ সাল থেকে এক হাতে মাউস (ডান) আরেক হাতে কী-বোর্ড নিয়ে বসে আছি, চোখের পাতা ফেলতে পারছিনা যদি একটা টার্ন মিস করি তাহলে গাড়ীটাই উল্টায়ে যাবে এই ভয়ে, winrar দিয়ে একটা একটা করে ভাইরাস এফেক্টেড ফাইল খুজে খুজে ফেলে দিয়ে পেন ড্রাইভ ওপেন করি,,,এই আমি, আমিও তো জানিনা। এই লজ্জা কোথায় রাখি!

নিজেকে অনেক ছোট করে ফেললাম; শুনতেই খারাপ লাগে। নিজেকে অনেক ছোট-খাটো করে তুলে ধরলাম; শুনতে ভালো লাগে। লেখতেও।

আমার নিজের সম্পর্কে এত ছোট ধারনা কখনই ছিলো না। কিন্তু প্রশ্নটাই তো আমাকে ভাবাচ্ছে। পৃথিবীর প্রথম কম্পিউটার ভাইরাস! ওটা ভাইরাসই ছিলো তো নাকি অন্য কিছু? আমরাতো আবার spyware, adware, password cracker, malware এবং এরকম আর যা কিছু আছে সবই এক নামে ট্যাগ করে রাখি- ভাইরাস। আরও সহজ করে বলা যায়, পিসিতে ইনস্টল করা এন্টিভাইরাস আমাদের যে

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

সব বিষয়ে হুশিয়ার করে তার সবই ভাইরাস (!)। মানব দেহের কিছু একটা হলে খুব সহজেই এর উত্তর পেয়ে যেতাম। তাহলে এখানে বসে কী-বোর্ড আর নিজের সাথে ধস্তা ধস্তি করতাম না। হয়ত ফেইসবুকে বসে ফ্রেন্ডদের সাথে আড্ডা অথবা নতুন কোন মুভির টরেন্ট ফাইল খুজে ডাউনলোড করতে দিয়ে একটা বই নিয়ে বসতাম।

মজার একটা ঘটনা বলি। আমি McAfee VirusScan Enterprise 8.0.0 ব্যবহার করি। অনেক আগের একটা ভার্সন, জানি। এর মধ্যে আরও কিছু বের হয়েছে, আমিও বেশ কিছু দিন ব্যবহার করেছি। কিন্তু পরে এটাতেই ফিরে আসলাম। "প্রথম প্রেম" অথবা "পুরাতন জিনিস পছন্দ" এ ধরনের কোন ধারনা আমার মধ্যে কখনই ছিলো না। আমি গোড়াও না। আমার আসলে C: ড্রাইভটাকে ব্লক করে রাখা দরকার যাতে ওখানে কোন কিছুই প্রবেশাধিকার না পায়। McAfee VirusScan Enterprise এর নতুন ভার্সনগুলোতেও এই সুবিধা ছিলো, কিন্তু যেহেতু আমার আগেরটা দিয়েই কাজ চলছে, সেহেতু পরেরটা নিয়ে পরে ভাবা যাবে ঠিক করে বসে আছি (rots ভাই, প্লিজ!)। তো একদিন আমি nero ইনস্টল করতে দিলাম, এমন সময় ইনস্টলেশন বন্ধ হয়ে "সাবধান বানী" শুরু। পাশে আমার এক ফ্রেন্ড বসে ছিলো। লাফ দিয়ে উঠলো, দোস্ত পিসিতে ভাইরাস। সত্যি সত্যি ভাইরাস এ্যফেক্ট করলেও আমার হৃদপিন্ড হয়ত এভাবে লাফ দিতো না। অহংকারটা আমার। সবসময় বলে বেড়াতাম আমার রুমে ভাইরাস ঢুকলেই আমি টের পেয়ে যাই, পিসি পর্যন্ত আসতে পারে না, পেনড্রাইভে ভাইরাস থাকলে ওটা দরজার বাইরে পেনড্রাইভ সহ আটকায় থাকে (লক্ষ্মন রেখা) ইত্যাদি ইত্যাদি। এজন্যই একটা চান্স পেয়ে দুটা কথা শোনানোর ব্যর্থ প্রচেষ্টা তখুনি বুঝে নিয়ে অবুঝ ছেলেটাকে ঠান্ডা করলাম , ভাইরাস না, ওটা আমার

McAfee।

-McAfee মানে?

-McAfee মানে হচ্ছে, McAfee দিয়ে C: ড্রাইভটাকে ব্লক করে রাখা। এতে C: ড্রাইভে .exe, .dll এবং এ ধরনের যে ফাইলগুলো আছে সেগুলো ঢুকতে পারে না। ঢুকতে পারে না মানে creation, modification, access ইত্যাদি। ওই গাধাটাকে এত কিছু একদিনে বললে শেষে আমার বাসায় আসাই বন্ধ করে দিবে যেটা আমার জন্য খুব খারাপ হবে। ওর কাছে আমি অনেক দিক দিয়েই ধরা।

সফটওয়ার মানেইতো ওটা C: ড্রাইভে কিছু একটা করবে যেটাকে আমরা বলি ইনস্টল। যদি ঢুকতেই না পারে তাহলে ওই কিছু একটা কিভাবে হবে? এখানেইতো ভাইরাসের কথাটা চলে আসে। ভাইরাসের কাজও একই রকম (কিছুটা)। উনাকেও C: ড্রাইভে ঢুকে কিছু একটা করতে হয়। এই কিছু একটা মানে ইনস্টলও হতে পারে এ্যফেক্টও হতে পারে। "আমার পিসিতে ভাইরাস ইনস্টল হয়েছে" শুনতেই হাস্যকর লাগে। "আমার পিসিতে ভাইরাস এ্যফেক্ট করেছে" শুনতে ভয় লাগে। কিন্তু এটাই প্রচলিত কথা, আমরা এটাই বলি। এখন যদি আমি না শুধরায় দিতাম তাহলে আমার ওই ফ্রেন্ডটা এই ব্যাপারটাকে ভাইরাস মনে করেই বসে থাকতো। বলে বেড়াতো, ভাইরাসের কারন সফটওয়ার ইনস্টল হচ্ছেনা, আগেরগুলাও কাজ করছে না এবং আরও কিছু কাল্পনিক সমস্যা "দোস্ত, পিসিটা একটু স্লো স্লো মনে হচ্ছে, না? ভাইরাসের কারনে নাকি?" "কারসারটা নড়ে না কেনো? ভাইরাসটার এত দুঃসাহস?"। হয়তো কোন একদিন রেগে-মেগে C: ড্রাইভ টাই ফরমেট দিয়ে দিতো, আমিই বলেছিলাম এটা করলে ভাইরাস সহ সবকিছুই ক্লিন হয়ে যায়।

এখন প্রশ্ন হচ্ছে, প্রথম ভাইরাস যেটা আসলে কি ছিলো তা আমি অন্তত জানিনা, তার নাম কি? তার চেয়েও গুরুত্বপূর্ন প্রশ্ন, কখন

এবং কবে থেকে বোঝা যাচ্ছিলো যে ওটা একটা ভাইরাস?

যখন আমরা বুঝতে শুরু করলাম যে কিছু একটা আছে যেটা কম্পিউটারের জন্য ক্ষতিকর, ফাইল নষ্ট করে দেয়, তথ্য গায়েব করে দেয় এবং আরো অনেক ঝামেলা করে তখন আমরা এটার নাম দিলাম ভাইরাস। যেহেতু ভাইরাস শব্দটার সাথে আমরা আগে থেকেই পরিচিত যা কিনা জীব বিজ্ঞানের ভাষা এবং "ক্ষতিসাধন" করাই যার কাজ সেহেতু ভাইরাস শব্দটাই যুক্তিযুক্ত মনে করা হল কম্পিউটারের জন্য। কিন্তু যখন আমরা ভাইরাস শব্দটা জানতামই না তখনও ভাইরাস ছিলো। আমরা জানতাম না, অসুস্থ হতাম, অনেকে মারাও যেতো। আমার এই সেক্টরে খুবই কম ধারনা কিন্তু মেডিকেলের যে কোন স্টুডেন্ট স্বাচ্ছন্দে বলে দিতে পারবে কোনটা মানব দেহের কিংবা জীব বিজ্ঞানের প্রথম ভাইরাস। মেডিকেলের স্টুডেন্ট ছাড়াও অনেকে হয়ত জানে কোনটা মানব দেহের প্রথম ভাইরাস, আমি জানিনা। তবে কম্পিউটারের ভাইরাস এতটা ভয়ংকর না আমাদের জন্য। কারন এটা আমরাই তৈরি করি। কখনও কাজের জন্য (কি কাজ সেটা আরেক ইতিহাস), কখনও অ'কাজের জন্য। জানতে হবে, কবে আমরা জানতে পারলাম যে আমাদেরই তৈরি করা একটা প্রগ্রাম যা কিনা খুব কাজের কিন্তু কোনও না কোন ভাবে অন্যদের জন্য ক্ষতিকর? অথবা, আমাদেরই তৈরি করা একটা প্রগ্রাম যা কিনা "ক্ষতিসাধন" করার জন্যই সর্বপ্রথম তৈরি করো হয়েছিলো?

এমনও হতে পারে, প্রথম ভাইরাস টা যে তৈরি করেছিলো সে তার উদ্দেশ্য হাসিল করে ফেলার পরে প্রগ্রামটা ডিলিট করে নিজেও কেটে পড়েছে। প্রথম ভাইরাস তৈরির যে আজীবন সম্মাননা, তার চেয়ে তার কাছে তখন তার উদ্দেশ্যটা সফল করাই বেশি গুরুত্বপূর্ন ছিলো। সে ক্ষেত্রে

T@NB!R 01738359555
তো আমরা কখনই জানতে পারবো না কোনটা প্রথম কম্পিউটার ভাইরাস।

আবার এমনএ হতে পারে, যখন আমরা জানলাম কিছু একটা আছে যা কিনা ভাইরাস তার আগেও হয়ত কিছু একটা ছিল যা ভাইরাসের মত ক্ষতি করে দিয়ে ইতিমধ্যে ইতিহাস। কিন্তু না জানার কারনে আমরা পরেরগুলা নিয়েই হা-হুতাশ করছি।

অতিতে যেটাই হয়ে থাকুক তা দিয়ে এখনকার সমস্যার সমাধান হবেনা বোঝা যাচ্ছে। তার চেয়ে ভালো যেটা আমরা সবাই জানি তা নিয়েই থাকি।

পৃথিবীর প্রথম কম্পিউটার ভাইরাস (ভাইরাস নামে কিছু একটা আছে এটা জানার পরে)-
Creeper virus, সর্বপ্রথম এটা ডিটেক্ট করা হয় ARPANET থেকে। ১৯৭১ সালে Bob Thomas এই প্রগ্রামটি তৈরি করে যা ARPANET'এর TENEX operating system কে আক্রমন করে।

BRAIN নামে একটা প্রগ্রাম তৈরি করে পাকিস্তানের Basit ও Amjad,দুই ভাই। অনেকের মতে নাকি এটাই পৃথিবীর প্রথম কম্পিউটার ভাইরাস (১৯৮৬)।

Elk Cloner নামে আরকটা ভাইরাসের কথা শোনা যায় যা কিনা ১৯৮১ সালে তৈরি করা হয়েছিলো Apple II কম্পিউটারের জন্য।

উপরের সবগুলোই আমার বিশ্বাস করতে ইচ্ছা হয়, কখনই বুঝে উঠতে পারি না কোনটাকে ছেড়ে কোনটাকে ধরি। সময়ের বিবেচনায় Creeper virus অগ্রাধিকার পেতে পারে কিন্তু Basit ও Amjad ভাই এর কাজটা অনেক বেশি জনপ্রিয়। এমনকি আমার বড় ভাই তার পরিষ্কার খাতায় নাকি এই নামটাও দেখেছিলো (সঠিক

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

T@NB!R 01738359555
উত্তরে টিক চিহ্ন দিন)। কিন্তু উনি এটা মার্ক করেননি। ওখানে Creeper virus এর কথা ছিলো কিনা জানিনা। তবে Elk Cloner এর কথা অনেকেই জানেনা (হয়ত), আমিও জানলাম একটু আগে Google এ সার্চ দিয়ে। তখন অবশ্য চিন্তাও করিনি সার্চ দিয়ে এত কিছু পাওয়ার পর মাথাটা এভাবে CRACK আর এখানে লিখতে বসে যাবো।

Viruses – Types and Examples

Types of viruses

Boot viruses: These viruses infect floppy disk boot records or master boot records in hard disks. They replace the boot record program (which is responsible for loading the operating system in memory) copying it elsewhere on the disk or overwriting it. Boot viruses load into memory if the computer tries to read the disk while it is booting.
Examples: Form, Disk Killer, Michelangelo, and Stone virus

Program viruses: These infect executable program files, such as those with extensions like .BIN, .COM, .EXE, .OVL, .DRV (driver) and .SYS (device driver). These programs are loaded in memory during execution, taking the virus with them. The virus becomes active in memory, making copies of itself and infecting files on disk.
Examples: Sunday, Cascade

Multipartite viruses: A hybrid of Boot and Program viruses. They infect program files and when the infected program is executed, these viruses infect the boot record. When you boot the computer next time the virus from the boot record loads in memory and then starts infecting

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

T@NB!R 01738359555
other program files on disk.
Examples: Invader, Flip, and Tequila

Stealth viruses: These viruses use certain techniques to avoid detection. They may either redirect the disk head to read another sector instead of the one in which they reside or they may alter the reading of the infected file's size shown in the directory listing. For instance, the Whale virus adds 9216 bytes to an infected file; then the virus subtracts the same number of bytes (9216) from the size given in the directory.
Examples: Frodo, Joshi, Whale

Polymorphic viruses: A virus that can encrypt its code in different ways so that it appears differently in each infection. These viruses are more difficult to detect.
Examples: Involuntary, Stimulate, Cascade, Phoenix, Evil, Proud, Virus 101

Macro Viruses: A macro virus is a new type of computer virus that infects the macros within a document or template. When you open a word processing or spreadsheet document, the macro virus is activated and it infects the Normal template (Normal.dot)-a general purpose file that stores default document formatting settings. Every document you open refers to the Normal template, and hence gets infected with the macro virus. Since this virus attaches itself to documents, the infection can spread if such documents are opened on other computers.
Examples: DMV, Nuclear, Word Concept.

Active X: ActiveX and Java controls will soon be the scourge of computing. Most people do not know how to control there web browser to enable or disable the various functions like playing sound or video and so, by default, leave a nice big hole in the security by allowing applets free run into there machine.

Email:tanbir_cox@yahoo.com
web: http://tanbir.99k.org

There has been a lot of commotion behind this and with the amount of power that JAVA imparts, things from the security angle seem a bit gloom.

These are just few broad categories. There are many more specialized types. But let us not go into that. We are here to learn to protect our self, not write a thesis on computer virus specification.

Tanbir Ahmad Razib

Mobile No:: 01738-359555//01916-457075//

E_Mail :: tanbir_cox@yahoo.com // tanbir.cox@gmail.com

Facebook:: http://www.facebook.com/tanbir.cox (srch: Tanbir Ahmad)

B.I.P. 01738359555

Web Site :: http://tanbir.99k.org